日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ８月２８日

出願番号
Application Number: 特願２００１－２５７７９４

出願人
Applicant(s): 三菱電機株式会社

２００１年 ９月１３日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　533298JP01

【提出日】　平成13年 8月28日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　7/00

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　前田　卓志

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　松下　雅仁

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　笹川　耕一

【特許出願人】

【識別番号】　000006013

【住所又は居所】　東京都千代田区丸の内二丁目２番３号

【氏名又は名称】　三菱電機株式会社

【代理人】

【識別番号】　100062144

【弁理士】

【氏名又は名称】　青山　葆

【選任した代理人】

【識別番号】　100086405

【弁理士】

【氏名又は名称】　河宮　治

【選任した代理人】

【識別番号】　100113170

【弁理士】

【氏名又は名称】　稲葉　和久

【手数料の表示】

【予納台帳番号】　013262

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　認証の選択システム、認証システム

【特許請求の範囲】

【請求項１】　被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部を備えることを特徴とする認証の選択システム。

【請求項２】　被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組合せを生成する組合せ生成部と、

前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部と

をさらに備えることを特徴とする請求項１に記載の認証の選択システム。

【請求項３】　前記目標性能を設定する目標性能設定部と、

選択する認証の制約条件を設定する制約条件設定部と

をさらに備え、

前記組合せ生成部は、前記制約条件に基づいて一の認証又は認証の組合せを生成し、

前記認証手段選択部は、前記目標性能を満たす一の認証又は認証の組合せの中から、前記制約条件に基づいて一の認証又は認証の組合せを選択することを特徴とする請求項１又は２に記載の認証の選択システム。

【請求項４】　前記制約条件は、認証手段の種類、認証手段の種類の優先順位、認証の組合せ方法、認証の組合せ方法の優先順位、組合せる認証の数、組み合わせる認証の数の優先順位、組合せの候補数、のうち少なくとも一つであることを特徴とする請求項３に記載の認証の選択システム。

【請求項５】　前記認証手段の認証性能を記憶しておく性能記憶部と、

前記認証手段による認証結果のログデータを解析し、前記認証手段の認証性能に反映させるログ解析部と

をさらに備えたことを特徴とする請求項１から４のいずれか一項に記載の認証の選択システム。

【請求項６】　前記性能記憶部は、登録者ごとの認証性能を記憶しているこ

とを特徴とする請求項５に記載の認証の選択システム。

【請求項７】　前記認証手段の認証性能は、被認証者が登録者本人である場合の入力データと登録データとの一致の度合いを示す照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうち少なくとも一つからなることを特徴とする請求項１から６のいずれか一項に記載の認証の選択システム。

【請求項８】　請求項１から７のいずれか一項に記載の一の認証又は認証の組み合わせを選択する前記認証の選択システムと、

被認証者の入力データを登録データと照合し、被認証者を認証する少なくとも一つの認証手段と、

を備え、

前記認証の選択システムで選択された前記一の認証又は認証の組み合わせによって、前記被認証者を認証することを特徴とする認証システム。

【請求項９】　被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと

を含むことを特徴とする認証の組み合わせの選択方法。

【請求項１０】　被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと

を含むことを特徴とする認証方法。

【請求項１１】　被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと

を含むことを特徴とするコンピュータで実行される認証の選択プログラム。

【請求項１２】　請求項１１に記載の前記認証の選択プログラムを格納したことを特徴とするコンピュータ読取可能な記録媒体。

【請求項１３】　被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと

を含むことを特徴とするコンピュータで実行される認証プログラム。

【請求項１４】　請求項１３に記載の前記認証プログラムを格納したことを特徴とするコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証手段を用いて被認証者を認証する認証システムに関する。

【０００２】

【従来の技術】

重要な機密事項に関して、接触できる人を制限して機密保持を行ったり、特定の部屋への入室者のチェックを行う方法には様々な方法がある。例えば、ＩＣカードや、ＩＤ、パスワード等の入力によって認証を行う方法がある。しかし、Ｉ

ＣカードやＩＤ、パスワード等は登録者本人以外の他人であっても使用することができるため、より厳密なセキュリティが求められる場合には充分ではない。

【０００３】

一方、他人に使用されることのない各個人に固有の指紋を用いた認証装置が知られている（特開２０００－７６４５０号公報）。この認証装置は、入力された指紋の種類と順番の組合せとを照合している。

【０００４】

【発明が解決しようとする課題】

上記認証装置による認証方法は、指紋による認証の機密性を高くするために指紋の入力回数を複数回にし、その入力順序が正しいか否かについても判断している。しかし、この方法では認証の機密性を高めることはできるが、ただ単に指紋の入力回数を複数回にしているだけであって、その結果どのくらいの認証精度が得られるか分からなかった。つまり、要求される認証精度があった時に、指紋の入力を何回にすれば必要な認証精度を確保できるか分からなかった。

【０００５】

そこで、本発明の目的は、認証に必要な目標性能を満たす認証手段を用いて被認証者が登録者であるか否か認証する認証システムを提供することである。

【０００６】

【課題を解決するための手段】

本発明に係る認証の選択システムは、被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部を備えることを特徴とする。

【０００７】

また、本発明に係る認証の選択システムは、前記認証の選択システムであって、被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組合せを生成する組合せ生成部と、

前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部と

をさらに備えることを特徴とする。

【０００８】

さらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記目標性能を設定する目標性能設定部と、

選択する認証の制約条件を設定する制約条件設定部と

をさらに備え、

前記組合せ生成部は、前記制約条件に基づいて一の認証又は認証の組合せを生成し、

前記認証手段選択部は、前記目標性能を満たす一の認証又は認証の組合せの中から、前記制約条件に基づいて一の認証又は認証の組合せを選択することを特徴とする。

【０００９】

またさらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記制約条件は、認証手段の種類、認証手段の種類の優先順位、認証の組合せ方法、認証の組合せ方法の優先順位、組合せる認証の数、組み合わせる認証の数の優先順位、組合せの候補数、のうち少なくとも一つであることを特徴とする。

【００１０】

また、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記認証手段の認証性能を記憶しておく性能記憶部と、

前記認証手段による認証結果のログデータを解析し、前記認証手段の認証性能に反映させるログ解析部と

をさらに備えたことを特徴とする。

【００１１】

さらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記性能記憶部は、登録者ごとの認証性能を記憶していることを特徴とする。

【００１２】

またさらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記認証手段の認証性能は、被認証者が登録者本人である場合の入力デ

ータと登録データとの一致の度合いを示す照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうち少なくとも一つからなることを特徴とする。

【００１３】

本発明に係る認証システムは、一の認証又は認証の組み合わせを選択する前記認証の選択システムと、

被認証者の入力データを登録データと照合し、被認証者を認証する少なくとも一つの認証手段と、

を備え、

前記認証の選択システムで選択された前記一の認証又は認証の組み合わせによって、前記被認証者を認証することを特徴とする。

【００１４】

本発明に係る認証の選択方法は、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと

を含むことを特徴とする。

【００１５】

本発明に係る認証方法は、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと

を含むことを特徴とする。

【００１６】

本発明に係るコンピュータで実行される認証の選択プログラムは、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと

を含むことを特徴とする。

【００１７】

本発明に係る認証の選択プログラムを格納したコンピュータ読取可能な記録媒体は、前記認証の選択プログラムを格納したことを特徴とする。

【００１８】

本発明に係るコンピュータで実行される認証プログラムは、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと

を含むことを特徴とする。

【００１９】

本発明に係る認証プログラムを格納したコンピュータ読取可能な記録媒体は、前記認証プログラムを格納したことを特徴とする。

【００２０】

【発明の実施の形態】

本発明の実施の形態に係る認証の選択システムと、認証システムについて、添付の図面を参照して以下に説明する。

【００２１】

実施の形態１．

本発明の実施の形態１に係る認証の選択システム及び認証システムについて説明する。この認証の選択システムは、図１のブロック図に示すように、コンピュータのメモリ２０上に読みこまれたプログラムとして、目標性能を設定する目標性能設定部２１と、選択する認証手段の制約条件を設定する制約条件設定部２２と、認証手段の認証性能を記憶しておく性能記憶部２３と、制約条件に基づいて認証手段を用いた認証の組合せを生成する組合せ生成部２４と、各認証の組合せごとの認証性能を演算する複合認証性能演算部２５と、制約条件に基づいて認証の組み合わせを選択する認証手段選択部２６とを備えている。この認証の選択システムでは、認証手段選択部２６で選択した認証手段を用いた認証の組合せによって被認証者を認証する。これによって目標性能を満たし、しかも制約条件に合う認証手段を用いた認証の組合せによって被認証者を認証することができる。なお、この認証システムは、上記各構成要素に限定されず、他の構成要素を含んでいてもよい。また、メモリ２０上に読みこまれた上記プログラムは、ハードディスク等の記録媒体上に記録されていてもよい。さらに、上記目標性能設定部２１と、制約条件設定部２２と、性能記憶部２３と、組合せ生成部２４と、複合認証性能演算部２５と、認証手段選択部２６とは、プログラムとしてではなく、ハードウエア的に実現してもよい。なお、この認証の選択システムの構成要素ではないが、被認証者を認証する認証手段としての認証手段１（指紋）１１及び認証手段２（虹彩）１２を用いている。また、上記ソフトウエアの機能実現のためのハードウエアとして、ＣＰＵ１３、記録媒体に格納されたプログラムを読み取る記録媒体ドライブ１４、入力装置１５、出力装置１６、メモリ２０等を備えていてもよい。

【００２２】

ここで、上記認証手段１１、１２について説明する。この認証手段１１、１２によって被認証者を認証する。この「認証」としては、例えば、被認証者の入力データと登録データとを照合して、被認証者が登録者本人であるか否かを判断する認証手続である。なお、これ以外の認証手続を行うものであってもよい。また、認証手段としては、指紋、顔、声、虹彩、掌形、署名などの生体情報と呼ばれ

る各被認証者がもつ身体的特徴あるいは動作によって認証する認証手段の他、パスワードやＩＣカード等の生体とは無関係な認証手段も用いることができる。好ましくは、指紋、顔、声、虹彩等の生体情報を用いて認証する認証手段である。生体情報を用いた認証の場合には、パスワードやＩＣカードの盗用のような他人による登録者への「なりすまし」を防止することができる。なお、「認証手段を用いた一の認証又は認証の組合せ」とは、少なくとも一つの認証手段を用いた少なくとも一つの認証を含んでいればよく、また、複数の認証手段を用いた認証の組合せに限られない。また、同一の認証手段を用いた認証を複数回組み合わせてもよい。さらに、各認証の組合せは、ＡＮＤ、ＯＲ、ＮＯＴ等の論理演算による場合の他、線形和や重み付き線形和等を用いてもよい。

【００２３】

次に、認証手段の認証性能について説明する。指紋や虹彩等の生体情報による認証を行う認証手段では、通常、登録データと入力データとの一致の度合を示す照合度という値が求められ、その照合度がある一定の閾値を越えるか否かで被認証者が本人であるかどうかを判断する。認証手段の認証性能は、例えば、被認証者が登録者本人であるのに、該登録者本人ではない他人と認証される誤認証（ＦＲ：false rejection）の割合であるＦＲＲ（false rejection rate）と、被認証者が該登録者本人ではない他人（以下、「他人」という）であるのに、該登録者本人と認証される誤認証（ＦＡ：false acceptance）の割合であるＦＡＲ（false acceptance rate）とによって表わされる。なお、複数の登録者がある場合には、被認証者はある登録者本人ではあるが、別の登録者本人と誤って認証される誤認証（ＦＡ）がある。このＦＲＲやＦＡＲは、設定する閾値によって変化するため、図４の（ａ）に示すように、閾値による関数として表わされる。また、ＦＲＲとＦＡＲとは、図４の（ａ）に示すように、トレードオフの関係にあり、一方を上げれば、もう一方は下がる性質がある。さらに、図４の（ｂ）は、被認証者が登録者本人である場合の本人照合度と、被認証者が該登録者本人でない他人である場合の他人照合度について、それぞれ照合度に対する頻度を示すグラフである。図４の（ａ）のＦＲＲ及びＦＡＲを閾値（照合度）で微分したものが図４の（ｂ）の本人照合度分布及び他人照合度分布に相当する。したがって、逆に

、図４の（ｂ）の本人照合度分布及び他人照合度分布を照合度について積分すると、図４の（ａ）のＦＲＲ、ＦＡＲにそれぞれ相当する。そこで、認証手段の認証性能として、図４の（ａ）又は（ｂ）のいずれのデータで記憶してもよい。なお、これ以外の方法で認証性能を定めてもよい。

【００２４】

認証システムが稼動を始める初期状態の場合など、蓄積されている実際の照合データが少ない場合には、単一の認証手段の認証性能は、使用する認証手段のセンサベンダが提供する認証性能特性を用いる。しかし、以下の手順で実際の照合データを用いて、単一の認証手段の性能を求めることが望ましい。各々の単一の認証手段の認証性能の算出は、実際の認証に先だってあらかじめ、図３のフローチャートに示すように、次の手順で行われる。

（１）あらかじめ、システム管理者によって入力装置１５から入力された登録者の登録データをＣＰＵ１３で受け取って、ハードディスク等の記録媒体等に登録しておく。

（２）次に、各認証手段１１、１２から被認証者の照合データをＣＰＵ１３で受け取る（１１１）。なお、次の手順は、照合データのうち、被認証者が登録者本人同士の照合データと、被認証者が互いに他人同士である照合データとに分けて行う。

（３－１）まず、被認証者が登録者本人である場合の照合データの処理手順を示す。この場合に、照合データのうち、同一の登録者本人の各照合ごとの照合データ間での照合をＣＰＵ１３で行って、本人照合度を算出する（１１２）。

（４－１）本人照合度の頻度分布をＣＰＵ１３で確率密度関数化する（１１３）。なお、ここでは照合度分布の表現方法として確率密度関数を用いたが、これに限られず、例えば、確率分布や正規分布等の標準的な分布関数で近似した場合の平均や分散等のパラメータを用いて表現してもよい。

（３－２）次に、被認証者が互いに他人同士である場合の照合データの処理手順を示す。この場合に、照合データのうち、他人同士の照合データ間での照合をＣＰＵ１３で行って、他人照合度を算出する（１１４）。

（４－２）他人照合度の頻度分布をＣＰＵ１３で確率密度関数化する（１１５）

。なお、この場合にも、上述のように照合度分布の表現方法は確率密度関数に限られず、例えば、確率分布や正規分布等の標準的な分布関数で近似した場合の平均や分散等のパラメータを用いて表現してもよい。

（５）本人照合度分布と他人照合度分布をそれぞれ性能記憶部２３に記憶する（１１６）。

以上の手順によって、例えば、図４の（ｂ）に示す本人照合度分布と、他人照合度分布を得ることができる。

【００２５】

また、図４の（ｂ）に示す本人照合度分布において、設定した閾値とＦＲＲとの関係について、図５の（ａ）を用いて説明する。被認証者の照合度ｘ１に対して、図５の（ａ）に示すように、閾値Ｔ１を設定すると、照合度ｘ１が閾値Ｔ１より低い斜線部では、被認証者が登録者本人であるのに該登録者本人ではない他人と認証されてしまう誤認証（ＦＲ）がある。この斜線部が本人照合度分布の全体に占める割合がＦＲＲである。同様に、図４の（ｂ）に示す他人照合度分布において、設定した閾値とＦＡＲとの関係について、図５の（ｂ）を用いて説明する。被認証者の照合度ｘ１に対して、図５の（ｂ）に示すように、閾値Ｔ１’を設定すると、照合度ｘ１が閾値Ｔ１’より高い斜線部は、被認証者が登録者本人ではない他人であるのに該登録者本人と認証されてしまう誤認証（ＦＡ）がある。また、複数の登録者がある場合、被認証者はある登録者本人ではあるが、別の登録者本人であると誤って認証される誤認証（ＦＡ）がある。この斜線部が他人照合度分布の全体に占める割合がＦＡＲである。なお、ここでは、斜線部を明確に示す説明の便宜上、閾値Ｔ１とＴ１’とはそれぞれ異なる値として示したが、実際には同一の閾値について、それぞれのＦＲＲとＦＡＲとを算出する。

【００２６】

この認証システムにおける認証動作は、図２のフローチャートに示す以下の手順で行われる。なお、ハードウエアの利用に関して、一般的なコンピュータを構成するＣＰＵ、メモリ、記録媒体ドライブ、記録媒体等を用いることができる。

（１）あらかじめ、システム管理者は、被認証者が登録者本人ではない他人であるのに、該登録者本人であると誤って認証する割合（ＦＡＲ）等の目標性能を目

標性能設定部２１で設定しておき、選択する認証の組合せに関する条件としての制約条件を制約条件設定部２２で設定しておく。この場合、ハードウエアの利用に関して、コンピュータのＣＰＵ１３ではシステム管理者によって入力装置１５を介して入力された目標性能と制約条件を受け取り、それぞれハードディスク等の記録媒体に記録しておく。

（２）次に、制約条件設定部２２で設定された制約条件に基づいて、認証手段を用いた一の認証又は認証の組合せを組合せ生成部２４で生成する（１０１）。この場合、ハードウエアの利用に関して、ＣＰＵ１３は記録媒体に記録された制約条件を読み込んで、一の認証又は認証の組合せを生成し、ハードディスク等の記録媒体に記録しておく。この時、生成される一の認証又は認証の組合せを図９の（ａ）の左列に示した。

（３）さらに、各認証の組み合わせごとの認証性能を複合認証性能演算部２５で演算し、各組合せごとに認証性能を性能記憶部２３に記憶する（１０３）。この場合、ハードウエアの利用に関して、ＣＰＵ１３で各認証の組合せごとの認証性能を演算し、記録媒体に記録している。

（４）そして、全ての認証と、全ての認証の組合せについて認証性能の演算を行ったか否かをＣＰＵ１３で判断する（１０３）。なお、全ての組合せについて演算していなければ、再度手順１０２を実行する。

（５）全ての認証と全ての認証の組合せについて演算を行い、記憶させた場合には、目標性能を満たす全ての認証と認証の組合せの中から認証手段選択部２６で制約条件に基づいて一の認証又は認証の組み合わせを選択する（１０４）。なお、ハードウエアの利用に関して、ＣＰＵ１３で一の認証又は認証の組合せを選択する。

以上の手順によって、目標性能を満たす一の認証又は認証の組み合わせを選択することができる。また、選択した一の認証又は認証の組合せによって、目標性能を確保して被認証者の認証を行うことができる。なお、目標性能の設定は、例えば、指紋や顔などのバイオメトリクスによる本人認証を部屋の入退室時に行う場合であれば、認証の対象とする複数の部屋のそれぞれについて設定しておいてもよい。この場合に、被認証者が入室を希望する部屋を選択した際に、認証手段

の選択を行う。

【００２７】

次に、上記フローチャートの各手順について説明する。まず、目標性能設定部２１で目標性能を設定する上記手順について説明する。目標性能の設定は、精度の高い認証を必要とする場合、例えば非常に重要な施設への入退室のドアの開閉についての認証には高い目標性能を設定し、一方、中程度の精度の認証を必要とするコンピュータへのログインの場合にはそれに見合った目標性能を目標性能設定部２１で設定すればよい。先にあげた例を用いれば、非常に重要な施設への入退室は、登録者本人が登録者でないと認証される割合のＦＲＲが高くとも、他人が誤って登録者と認証される割合のＦＡＲを低く抑えたい。この場合、目標性能としては（ＦＲＲ、ＦＡＲ）＝（３．０％、０．００１％）等のようにシステム管理者が設定する。一方、コンピュータのログインでは、それほどセキュリティを重視せず利便性を重視するのであれば、目標性能としては（ＦＲＲ、ＦＡＲ）＝（０．１％、０．１％）等のようにシステム側によって設定する。

【００２８】

また、制約条件設定部２２で選択する認証の組合せに関する制約条件を設定する上記手順について説明する。ここで制約条件とは、認証の組合せの選択にあたって、用いる認証手段の種類やその優先順位、複数の認証手段を用いた認証を組合せる最大数、さらに、認証を組合せる方法やその優先順位等の条件である。例えば、重要施設のドアであれば、制約条件として、認証手段の候補を指紋と虹彩とし、最大の組合せ数を４、組合せ方法をＡＮＤと設定することができる。また、コンピュータログインであれば、制約条件として認証手段の候補は指紋と顔と声とし、最大の組合せ数は３、組合せ方法はＡＮＤ、ＯＲ、重み付き線形和等と設定することができる。

【００２９】

さらに、図２の各組み合わせの複合認証性能を演算し、記憶する手順１０２について、図６のフローチャートを用いて説明する。

（１）まず、認証手段を用いた認証の組合せについて、ＣＰＵ１３で複合認証モデルを作成する（１２１）。なお、この手順１２１については後述する。

（２）次に、各認証手段の認証性能を性能記憶部２３から読み込む（１２２）。ハードウエアの利用に関しては、各認証手段の認証性能を記録媒体から読みこむ。

（３）各認証手段の照合度ｘ１、ｘ２の閾値Ｔ１、Ｔ２の初期値を設定する（１２３）。例えば、照合度の範囲が０から１００と設定している場合には、初期値（Ｔ１、Ｔ２）＝（０、０）と設定してもよい。

（４）設定した閾値Ｔ１、Ｔ２による認証性能（ＦＲＲ、ＦＡＲ）を算出する（１２４）。ハードウエアの利用としては、ＣＰＵ１３で上記認証性能を算出する。

（５）設定した閾値Ｔ１、Ｔ２の複合認証性能を記憶する（１２５）。ハードウエアの利用としては、記録媒体に記録する。

（６）閾値Ｔ１、Ｔ２の設定を全範囲で行ったか否かをＣＰＵ１３で判断する（１２６）。閾値の設定が全範囲で行われていなかった場合には閾値を更新し（１２８）、手順１２４に戻って複合認証性能を算出する。この閾値の更新は、例えば、いずれか一方の閾値を１づつ増していってもよい。また、その刻み幅は、各認証手段で得られる照合度の精度に応じて設定すればよい。例えば、照合度の制度が小数点以下一桁であれば、０．１刻みに、小数点二桁の精度があれば０．０１刻みで変化させればよい。

（７）閾値の設定を全範囲で行った後、目標性能を満たす閾値の範囲をＣＰＵ１３で探索する（１２７）。この手順については後述する。

以上の手順によって、目標性能を満たす各組合せの認証性能を演算し、記憶させることができる。

【００３０】

ここで、制約条件として、例えば、認証手段の種類に関して指紋を優先し、認証手段を用いた認証の組合せ数が少ない組合せを優先するという条件がある場合には、認証手段選択部によって、図９の（ａ）に示す関係の中から条件に合わせて優先度の高い順番に並べ替え、最終的な認証の組み合わせとして、図９の（ｂ）のような組合せを選択する。これによって、目標性能を満たす認証の組合せの中から上記制約条件を満たす認証の組合せを選択することができる。なお、図９

では、簡略化するために、各認証の組合せについて指紋の照合度の閾値（Ｔ１）と虹彩の照合度の閾値（Ｔ２）とを一組しか示していない。しかし、実際には、目標性能を満たすための閾値の組合せ（Ｔ１，Ｔ２）は、これ以外にも所定の範囲にわたって取り得る場合がある。また、一定の刻み幅で設定する場合、その組合せは多数存在し、これらを用いることができる。

【００３１】

次に、上記図６の手順について、認証手段を用いた認証の組合せが「指紋と虹彩の重み付き線形和」の例によって説明する。

（１）まず、各認証手段の認証性能を読み込む。この例では、認証手段としての指紋による本人照合度の確率密度関数ｆ１（ｘ１）と、他人照合度分布の確率密度関数ｇ１（ｘ１）および虹彩の本人照合度の確率密度関数ｆ２（ｘ２）、他人照合度分布の確率密度関数ｇ２（ｘ２）を性能記憶部２３から読み出す。ハードウエアの利用としては、記録媒体から読み出す。ここで、添え字の１および２は、それぞれ認証手段としての指紋および虹彩を意味しており、ｘ１、ｘ２は、それぞれ認証手段として指紋および虹彩による照合度を意味する。

（２）この認証の組合せ「指紋と虹彩の重み付き線形和」について、複合認証性能モデルを作成する。まず、下記式に示す重み付き線形和に対応した新しい変数ｚを設定する。

【数１】

$$z = weightsum(x1 - T1, x2 - T2) = w1(x1 - T1) + w2(x2 - T2) \qquad (1)$$

【００３２】

この変数ｚは、この認証の組合せにおいて、０または正の値をとる場合には被認証者は登録者本人であると判断し、負の値をとる場合には被認証者は他人であると判断する変数である。また、変数ｚを構成するweightsum()関数は、各引数にそれぞれ重み係数をかけて線形和の演算を行う関数であり、ｗ１およびｗ２はそれぞれ指紋の照合度ｘ１および虹彩の照合度ｘ２に対する重み係数である。このｗ１、ｗ２は、それぞれの認証手段に対する認証の依存度を表わしたパラメータである。

【００３３】

次に、被認証者が登録者本人である場合の変数ｚの確率密度関数をＦ（ｚ、Ｔ１、Ｔ２）と表記し、被認証者が他人である場合のｚの確率密度関数をＧ（ｚ、Ｔ１、Ｔ２）と表記する。それぞれの認証手段による認証結果が互いに独立である場合には、式（１）のｚについての確率密度関数は、それぞれの確率密度関数の積で表わすことができるので、それぞれ下記式（２）及び式（３）で表わすことができる。

【数２】

$$F(z,T1,T2)=\int_{-\infty}^{+\infty} f1(x'1)f2(x'2)dx'1=\int_{-\infty}^{+\infty} f1(x'1)f2((z-w1\cdot x'1)/w2)dx'1 \qquad (2)$$

【数３】

$$G(z,T1,T2)=\int_{-\infty}^{+\infty} g1(x'1)g2(x'2)dx'1=\int_{-\infty}^{+\infty} g1(x'1)g2((z-w1\cdot x'1)/w2)dx'1 \qquad (3)$$

なお、式（２）および式（３）では、ｘ’１＝ｘ１－Ｔ１、ｘ’２＝ｘ２－Ｔ２という変数変換を行って、それぞれｘ’１、ｘ’２の関数として表わしている。また、ここでは各認証手段による認証結果について互いに独立であると想定したが、それぞれの認証結果の間に一定の相関関係を有する場合には、相関係数等を考慮して構成することができる。

【００３４】

上記式（１）のように設定した変数ｚにおいて、ｚが０もしくは正の時、登録者本人と判断し、ｚが負の場合に他人と判断するものとする。これにより、図６の上記手順１２４において、被認証者が登録者本人であるのに、該登録者本人でないと判断される割合ＦＲＲと、被認証者が他人であるのに登録者本人であると判断される割合ＦＡＲとは、Ｆ（ｚ、Ｔ１、Ｔ２）およびＧ（ｚ、Ｔ１、Ｔ２）を用いて下記式（４）及び式（５）で表わされる。

【数４】

$$FRR(T1,T2)=\int_{-\infty}^{0} F(z,T1,T2)dz \qquad (4)$$

【数５】

$$FAR(T1,T2)=\int_0^{+\infty}G(z,T1,T2)dz \qquad (5)$$

【００３５】

上記式（４）及び式（５）によって以上のように複合認証の方法に従って変数ｚを設定すれば、登録者本人のｚの確率密度関数Ｆ（ｚ、Ｔ１、Ｔ２）および他人のｚの確率密度関数Ｇ（ｚ、Ｔ１、Ｔ２）が決定でき、Ｆ（ｚ、Ｔ１、Ｔ２）が負となる条件からＦＲＲの、Ｇ（ｚ、Ｔ１、Ｔ２）が正となる条件からＦＡＲの複合認証性能モデルを作成することができる。

【００３６】

また、「指紋と虹彩とのＡＮＤ認証」を考える。この場合には、ＡＮＤ演算であるので、認証手段として指紋によって登録者本人と認証し、かつ、虹彩によって登録者本人と認証された場合にのみ被認証者は登録者本人と認証される。この場合に、被認証者が登録者本人であるか否かを判断する上記変数は、下記式（６）で表わされる。すなわち、ＡＮＤ認証の場合は、上記重み付き線形和認証の場合の式（１）を式（６）に置き換えることで複合認証性能モデルを作成することができる。

【数６】

$$z=\min(x1-T1,x2-T2) \qquad (6)$$

【００３７】

ここで、ｍｉｎ（）は引数の最小値を求める関数である。上記と同様に、式（６）で表わされる変数ｚが０又は正の値をとる場合には登録者本人と判断し、負の場合には他人と判断する。したがって、被認証者が登録者本人であるのに、該登録者本人でないと誤って認証される場合（ＦＲ）は、指紋と虹彩とによる照合度ｘ１、ｘ２の少なくとも一方がそれぞれの閾値Ｔ１、Ｔ２を越えなかった場合に発生する。一方、被認証者が他人の場合に該登録者本人と誤って認証される場合（ＦＡ）は、指紋と虹彩との照合度ｘ１、ｘ２の両方がそれぞれの閾値Ｔ１、Ｔ２を越えた場合に発生する。なお、登録者が複数ある場合には、被認証者がある登録者本人であるが、別の登録者本人と誤って認証される場合（ＦＡ）がある

。

【００３８】

さらに、「指紋と虹彩とのＯＲ認証」を考える。この場合には、ＯＲ演算であるので、認証手段として指紋によって登録者本人と認証するか、または、虹彩によって登録者本人と認証された場合に被認証者は登録者本人と認証される。この場合に、被認証者が登録者本人であるか否かを判断する上記変数は、下記式（７）で表わされる。すなわち、ＯＲ認証の場合は、上記重み付き線形和認証の場合の式（１）を式（７）に置き換えることで複合認証性能モデルを作成することができる。

【数７】

$$z = \max(x1 - T1, x2 - T2) \qquad (7)$$

【００３９】

ここで、ｍａｘ（）は引数の最大値を求める関数である。上記と同様に、式（７）で表わされる変数ｚが０又は正の値をとる場合には登録者本人と判断し、負の場合には他人と判断する。したがって、被認証者が登録者本人であるのに、該登録者本人でないと誤って認証される場合（ＦＲ）は、指紋と虹彩とによる照合度ｘ１、ｘ２の両方がそれぞれの閾値Ｔ１、Ｔ２を越えなかった場合に発生する。一方、被認証者が他人の場合に該登録者本人と誤って認証される場合（ＦＡ）は、指紋と虹彩との照合度ｘ１、ｘ２の少なくとも一方がそれぞれの閾値Ｔ１、Ｔ２を越えた場合に発生する。なお、登録者が複数ある場合には、被認証者がある登録者本人であるが、別の登録者本人と誤って認証される場合（ＦＡ）がある。また、他の論理演算等や、これ以外の複合認証方法においても、式（１）に示す変数ｚの定義を変更することによって、その複合認証性能モデルを作成することができる。

【００４０】

次に、図６の上記手順１２７について、図７のフローチャートを用いて説明する。

（１）まず、閾値の初期値を設定する（１３１）。この閾値の初期値の設定は、上記図６の手順１２３と同様に行うことができる。

（２）設定した閾値に対応する複合認証性能（ＦＲＲ，ＦＡＲ）を記録媒体から読み込む（１３２）。

（３）読みこんだ認証性能が目標性能（ＦＲＲ、ＦＡＲ）を満たすか否かを判断する（１３３）。例えば、指紋と虹彩の組み合わせにおいて、目標性能として（ＦＲＲ，ＦＡＲ）＝（３．０％、０．００１％）と設定されている場合、設定された閾値Ｔ１、Ｔ２に対応して読みこまれた認証性能（ＦＲＲ、ＦＡＲ）を上記目標性能のそれぞれの値と比較することによって目標性能を満たすか否かの判断をＣＰＵ１３で行う。

（４）手順１３３で設定した閾値による認証性能の値が目標性能を満たしていると判断された場合、その場合の閾値を記録媒体に記憶させる（１３４）。一方、手順１３３で設定した閾値による認証性能の値が目標性能を満たしていないとＣＰＵ１３で判断された場合には、この手順１３４を飛ばして次の手順１３５に移る。

（５）次いで、閾値の設定を全範囲で行ったかＣＰＵ１３で判断する（１３５）。閾値の設定を全範囲で済ませていた場合には終了する。

（６）一方、手順１３５で閾値の設定が済んでいない範囲があれば閾値の更新をして（１３６）、手順１３２に戻る。

【００４１】

さらに、図２の目標性能を満たす認証の組合せの中から、制約条件に基づいて認証の組合せを選択する手順１０４について、図８及び図９の（ａ）、（ｂ）を用いて説明する。

（１）制約条件に基づいて生成された各認証の組み合わせについて、目標性能を満たす閾値を記録媒体から読みこむ（１４１）。例えば、図９の（ａ）に示す表のように、認証の組合せと目標性能を満たす閾値との組合せである。

（２）目標性能を満たす閾値があるか否かをＣＰＵ１３で判断する（１４２）。

（３）手順１４２で目標性能を満たす閾値がある場合には、その認証の組合せの種類と閾値とを記録媒体に記憶する（１４３）。一方、手順１４２で目標性能を満たす閾値がない場合には、手順１４３を迂回する。

（４）全ての組合せを読みこんだか否かをＣＰＵ１３で判断する（１４４）。読

みこんでいない組合せがあれば、対象の組合せを次の組合せに更新して（１４７）、手順１４１へ移る。

（５）一方、手順１４４で全ての組合せについて読みこんだとＣＰＵ１３で判断した場合には、目標性能を満たす閾値が存在する組合せを制約条件の優先順位に基づいて配列する（１４５）。例えば、制約条件として、認証手段に指紋を用いた場合の優先順位が高い場合には、図９の（ａ）に挙げられている組合せのうち、図９の（ｂ）に示すように配列される。

（６）配列の先頭にある認証の組合せをＣＰＵ１３で選択する（１４６）。なお、この認証の組合せの選択に関しては、単一の制約条件によって配列する場合に限られず、複数の制約条件によって配列し、選択してもよい。

【００４２】

なお、この認証の選択システムでは、認証手段として指紋と虹彩の例を挙げたが、他の認証手段であっても、ｆ１（）、ｆ２（）が他の認証手段の確率密度関数に置き換わるだけであり、同様の複合認証性能モデルを適用できる。また、認証を組み合わせる数が３以上の場合にも、それぞれの確率密度関数がｆ１（）、ｆ２（）、ｆ３（）と順次増えるだけであり、同様のモデルを適用できる。

【００４３】

さらに、この実施の形態１では、認証手段として指紋、虹彩等の例をあげたが、これに限られず種々の認証手段を用いることができる。また、認証手段を用いた認証の組合せ最大数として４の例をあげたが、これに限られず所望の数を設定してもよい。さらに、認証の組合せ方法として重み付き線形和、ＡＮＤ演算、それにＯＲ演算の例をあげたが、これに限られず、種々の演算方法を用いてもよい。

【００４４】

また、この認証の選択システムをコンピュータ上で実行する認証の選択プログラムは、図２に示すように、下記手順からなる。

（１）あらかじめ、システム管理者によって入力装置１５から入力された登録者本人を登録者でないと誤って認証する割合（ＦＲＲ）等の目標性能をコンピュータで受け取り、記録媒体に記録しておき、システム管理者によって入力装置１５

から入力された選択する認証の組合せに関する条件としての制約条件を受け取り、記録媒体に記録しておく。

（２）次に、設定した制約条件に基づいて、ＣＰＵ１３等で認証の組合せを生成する（１０１）。

（３）さらに、各組み合わせごとの認証性能をＣＰＵ１３で演算し、各組合せごとの認証性能を記録媒体等に記憶する（１０３）。

（４）そして、すべての組合せについて認証性能の演算を行ったか否かをＣＰＵ１３で判断する（１０３）。なお、全ての組合せについて演算していなければ、再度手順１０２を実行する。

（５）全ての組合せについて演算を行い、記憶させた場合には、上記認証の組合せの中から制約条件に基づいて認証の組み合わせをＣＰＵ１３で選択する（１０４）。

以上の手順によって、この認証の選択システムをコンピュータ上で実行し、目標性能を満たす認証の組合せを選択し、目標性能を確保して被認証者の認証を行うことができる。

【００４５】

さらに、上記認証の選択プログラムをコンピュータで読み取ることができる記録媒体に格納してもよい。このようにコンピュータ読取可能な記録媒体に格納することによって可搬性を備え、この認証の選択システムを稼動させることが容易に行うことができる。また、この認証の選択プログラムは、電子通信回線を通じて搬送することができるので、さらに遠隔地においても容易に実行させることができる。

【００４６】

なお、上記コンピュータ読取可能な記録媒体としては、フレキシブルディスク、ハードディスク、等の磁気記録媒体、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ等の光記録媒体、ＭＯ、ＭＤ等の光磁気記録媒体、ＥＥＰＲＯＭ、ＤＲＡＭ、フラッシュメモリ等の半導体記録媒体を用いることができる。また、これらの記録媒体に格納された認証の選択プログラムは記録媒体読取装置で読み取られ、コンピュータ上で実行される。

【００４７】

次に、この認証システムについて説明する。この認証システムは、図１のブロック図に示すように、上記認証の選択システムと、被認証者を認証する認証手段としての認証手段１（指紋）１１及び認証手段２（虹彩）１２とを備えている。また、この認証システムは、さらにＣＰＵ１３、記録媒体に格納されたプログラムを読み取る記録媒体ドライブ１４、入力装置１５、出力装置１６、メモリ２０等を備えている。なお、この認証システムは、上記各構成要素に限定されず、他の構成要素を含んでいてもよい。この認証システムの構成要素である認証の選択システムは、上述の通り、メモリ２０上に読みこまれたプログラムとして、ハードウエアであるＣＰＵ１３等によってその機能を実現している。この認証システムでは、認証の選択システムによって選択された認証手段を用いた一の認証又は認証の組合せによって、各認証手段１１、１２を用いて被認証者を認証する。これによって目標性能を満たし、しかも制約条件に合う認証手段を用いた認証の組合せによって被認証者を認証することができる。

【００４８】

次に、この認証システムにおける認証方法について、図１１のフローチャートを用いて説明する。この認証システムの認証方法は、実施の形態１に係る認証の選択方法の手順を含んでいる。そのため、この認証方法は、図２に示す認証の選択方法の手順１０４まで同一である。さらに、この手順１０４の後、手順１０５では、選択した認証手段を用いた一の認証又は認証の組み合わせを用いて、被認証者を認証している（１０５）。

【００４９】

また、この認証方法をコンピュータ上で実行する認証プログラムは、図１１に示すように、下記手順からなる。

（１）あらかじめ、システム管理者によって入力装置１５から入力された登録者本人を登録者でないと誤って認証する割合（ＦＲＲ）等の目標性能をコンピュータで受け取り、記録媒体に記録しておき、システム管理者によって入力装置１５から入力された選択する認証の組合せに関する条件としての制約条件を受け取り、記録媒体に記録しておく。

（２）次に、設定した制約条件に基づいて、ＣＰＵ１３等で認証の組合せを生成する（１０１）。

（３）さらに、各組み合わせごとの認証性能をＣＰＵ１３で演算し、各組合せごとの認証性能を記録媒体等に記憶する（１０３）。

（４）そして、すべての組合せについて認証性能の演算を行ったか否かをＣＰＵ１３で判断する（１０３）。なお、全ての組合せについて演算していなければ、再度手順１０２を実行する。

（５）全ての組合せについて演算を行い、記憶させた場合には、上記認証の組合せの中から制約条件に基づいて認証の組み合わせをＣＰＵ１３で選択する（１０４）。

（６）選択した認証の組合せによって被認証者の認証を行う（１０５）。

以上の手順によって、この認証システムをコンピュータ上で実行し、目標性能を満たす認証を選択し、目標性能を確保して被認証者の認証を行うことができる。

【００５０】

さらに、上記認証プログラムをコンピュータで読み取ることができる記録媒体に格納してもよい。このようにコンピュータ読取可能な記録媒体に格納することによって可搬性を備え、この認証システムを稼動させることが容易に行うことができる。また、この認証プログラムは、電子通信回線を通じて搬送することができるので、さらに遠隔地においても容易に実行させることができる。

【００５１】

なお、上記コンピュータ読取可能な記録媒体としては、フレキシブルディスク、ハードディスク、等の磁気記録媒体、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ等の光記録媒体、ＭＯ、ＭＤ等の光磁気記録媒体、ＥＥＰＲＯＭ、ＤＲＡＭ、フラッシュメモリ等の半導体記録媒体を用いることができる。また、これらの記録媒体に格納された認証プログラムは記録媒体読取装置で読み取られ、コンピュータ上で実行される。

【００５２】

実施の形態２．

本発明の実施の形態２に係る認証の選択システム及び認証システムについて説明する。まず、この認証の選択システムについて説明する。この認証の選択システムは、実施の形態１に係る認証の選択システムと比較すると、図１１のメモリ２０に示すように、実際に認証を行っていく中で蓄積するログデータを解析するログ解析部２７を備えている点で相違する。このログ解析部２７によって実際の認証結果に対応して、それぞれの認証手段の認証性能に動的に反映させることができる。なお、ログ解析部２８はＣＰＵ１３上で実行されるプログラムによって実現される。

【００５３】

この認証の選択システムは、あらかじめ性能記憶部２３に記憶されている各認証手段１１、１２の認証性能（ＦＲＲ、ＦＡＲ）について、実際の認証で得られるログデータを解析し、各認証手段の認証性能を更新している。例えば、ある認証で認証手段として指紋が用いられた場合、このログデータとして照合時の入力データを残しておく。ログ解析部２８は、残された照合時の入力データを用いて、被認証者が登録者本人と認証された場合と、被認証者が他人と認証された場合とに分類する。次いで、登録者本人同士のデータ相互の照合による本人照合度分布と、他人同士のデータ相互の照合による他人照合度分布とを算出することができる。このように認証が行われるごとに各認証手段による実際の認証実績が記憶されていくため、その結果を統計処理し、既存の各認証手段の認証性能を更新することができる。このように実際の認証実績を各認証手段の認証性能に反映させることによって、より実際の認証の実性能に基づいて認証を選択できる。

【００５４】

このログデータを解析し、各認証手段による認証性能へ反映する手順の詳細について、図１２及び図１３のフローチャートを用いて以下に説明する。まず、被認証者が登録者本人と認証されたログデータを本人照合度分布に反映させる場合について、図１２を用いて以下に説明する。

（１）ログデータの中で、登録者本人と認証された照合データ、照合度を記録媒体からそれぞれ順に読み込む（１５１）。

（２）照合度は所定のデータ反映用閾値以上であるか否かをＣＰＵ１３で判断す

る（１５２）。

（３）上記手順１５２で照合度が所定の反映用閾値以上の場合には、その照合データを登録者本人データとして記録媒体に記憶する（１５３）。上記手順１５２で照合度が所定値より低い場合には反映用としては用いないこととする。この場合に、本人と判定する閾値よりも高いデータ反映用閾値を設定し、照合度が上記のデータ反映用閾値を越えたデータのみを反映用のデータとして用いるのが好ましい。これによってデータ反映の信頼度を高めることができる。

（４）次に、対象となるログデータを全て読み込んだか否かをＣＰＵ１３で判断する（１５４）。読みこんでいないログデータがあれば手順１５１に戻って読みこむ。

（５）登録者ごとに登録者本人とされた各照合データ間についてＣＰＵ１３によって相互に照合を行って、本人照合度を算出する（１５５）。

（６）ログデータによる本人照合度の頻度分布を算出する（１５６）。

（７）全登録者に関する既存の本人照合度分布にログデータによる本人照合度分布を反映させ、本人照合度分布を更新する（１５７）。ハードウエアの利用としては、記録媒体から読みこんだ本人照合度分布に上記ログデータによる本人照合度分布を追加し、更新する。これによって、本人照合度の確率密度関数の積分であるＦＲＲにも反映させることができる。

【００５５】

また、被認証者が登録者本人と認証されたログデータを他人照合度分布に反映させる場合について、図１３を用いて以下に説明する。

（１）ログデータの中で、登録者本人と認証された照合データ、照合度を記録媒体からそれぞれ順に読み込む（１６１）。

（２）照合度が所定のデータ反映用閾値以上であるか否かをＣＰＵ１３で判断する（１６２）。

（３）上記手順１６２で照合度が所定の反映用閾値以上の場合には、その照合データを登録者本人データとして記録媒体に記憶する（１６３）。上記手順１６２で照合度が所定値より低い場合には反映用としては用いないこととする。この場合に、登録者本人と判定する閾値よりも高いデータ反映用閾値を設定し、照合度

が上記のデータ反映用閾値以上のデータのみを反映用のデータとして用いるのが好ましい。これによってデータ反映の信頼度を高めることができる。

（４）次に、対象となるログデータを全て読み込んだか否かをＣＰＵ１３で判断する（１６４）。読みこんでいないログデータがあれば手順１６１に戻って読みこむ。

（５）登録者本人とされた照合データについて、互いに異なる他人の照合データ間についてＣＰＵ１３で相互に照合を行って、他人照合度を算出する（１６５）。

（６）ログデータによる他人照合度の頻度分布を算出する（１６６）。

（７）全登録者に関する既存の他人照合度分布にログデータによる他人照合度分布を反映させ、他人照合度分布を更新する（１６７）。ハードウエアの利用に関しては、記録媒体から読みこんだ他人照合度分布に上記ログデータによる他人照合度分布を追加して更新している。これによって、他人照合度の確率密度関数の積分であるＦＡＲにも反映させることができる。

【００５６】

なお、このログ解析による反映は、ログが増えるごとに行ってもよく、あるいは所定数のログが蓄積された場合に行ってもよい。また、所定時間ごと、例えば、１日１回行ってもよい。さらに、ログからの照合データ抽出は、前回の処理以降に記録されたログについて行えばよい。また、相互に照合するデータとしては、新たなログのデータのみで行ってもよく、あるいは古いデータを含めて相互に照合してもよい。

【００５７】

次に、この認証システムについて説明する。この認証システムは、実施の形態１に係る認証システムと比較すると、図１１に示すように、上記認証の選択システムに関する相違と同様に、メモリ２０内にログ解析部２７を備えている点で相違する。また、上記認証の選択システムをコンピュータ上で実行するためのハードウエアとして、実施の形態１に係る認証システムと同様に、認証手段１１、１２を備えるとともに、ＣＰＵ１３、記録媒体ドライブ１４、入力装置１５、出力装置１６を備えている。

【００５８】

実施の形態３．

本発明の実施の形態３に係る認証の選択システムについて説明する。この認証の選択システムは、各々の認証手段の認証性能を全登録者でのデータとしてのみ有している実施の形態１及び２に係る認証の選択システムと比較すると、各々の認証手段の認証性能を各登録者ごとのデータとして保存している点で相違する。これによって、登録者をＩＤ等で特定して被認証者の認証を行う場合には、各登録者ごとにより最適な認証の組合せ、閾値等の認証条件を選択することができる。

【００５９】

また、上記実施の形態２に係る認証の選択システムに示す場合と同様に、実際の認証のログデータを解析して、その結果を各認証手段の認証性能に反映させることができる。この場合には、各登録者ごとの本人照合度およびＦＲＲ、他人照合度およびＦＡＲを算出し、既存の各登録者ごとの本人照合度分布およびＦＲＲ、他人照合度分布およびＦＡＲを更新する。これによって実際の認証結果に基づいた本人照合度分布、他人照合度分布を用いて特定登録者ごとの最適な認証を選択することができる。なお、特定の登録者についての他人照合度分布とは、その登録者本人のデータとその登録者以外の他人との間の相互に照合された照合度を意味している。また、この場合には、あらかじめ認証の対象となる登録者が特定されていることが前提となる。

【００６０】

なお、このログ解析による反映は、ログが増えるごとに行ってもよく、あるいは所定数のログが蓄積された場合に行ってもよい。また、所定時間ごと、例えば、１日１回行ってもよい。さらに、ログからの照合データ抽出は、前回の処理以降に記録されたログについて行えばよい。また、相互に照合するデータとしては、新たなログのデータのみで行ってもよく、あるいは古いデータを含めて相互に照合してもよい。

【００６１】

実施の形態４．

本発明の実施の形態４に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態１に係る認証の選択システムと比較すると、図１４に示すように、制約条件として認証手段の種別の優先順位を設定する点で相違する。上記実施の形態１で示したように、目標性能を満たす一の認証又は認証の組合せは複数存在する場合がある。この認証の選択システムでは、制約条件設定部２２で認証手段の種別の優先順位を設定している。これによって適切な一の認証又は認証の組合せを選択することができる。なお、この制約条件としては、認証手段の種類、その優先順位、組合せる最大数、組み合わせる数の優先順位、認証の組合せ方法、組合せ方法の優先順位、認証の組合せの候補数、などを設定することができる。また、認証手段の種類の優先順位として、認証手段の各種類の特性、例えば、処理時間、処理コスト、使用エネルギー等によってそれぞれことなる優先順位を決めてもよい。この場合、処理時間の速さに基づく認証手段の種類の優先順位としては、例えば、指紋が最も処理時間が速く、２番目に顔、３番目に虹彩である。

【００６２】

次に、図１４に示す認証手段の種類の優先順位によって、各組み合わせを配列する場合の手順を以下に示す。

（１）まず、認証の組合せの候補が複数ある場合には、制約条件である図１４の認証手段の優先順位に基づいて、認証手段選択部２６において一の認証及び認証の組合せを並べ替える。この並べ替えでは、図１４の認証手段の優先順位として、指紋の優先順位が最も高いので、まず認証手段に指紋を含む一の認証又は認証の組合せを選ぶ。次に、優先順位が２番目の虹彩を含む一の認証又は認証の組合せを選ぶ。図９の（ａ）に示す一の認証又は認証の組合せと目標性能を満たす閾値との関係があれば、図１５の表に示すように並び替えられる。

（２）次いで、最も優先順位が高い一の認証又は認証の組合せが最終候補としてＣＰＵ１３によって選択される。

以上のようにして、認証手段の種別の優先順位を与えることによって最終候補を絞りこむことができる。

【００６３】

実施の形態５．

本発明の実施の形態５に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態４に係る認証の選択システムと比較すると、制約条件として、認証の組合せ方法（演算方法）の優先順位及び組合せる認証の数の優先順位を設定する点で相違する。この制約条件によって、目標性能を満たす認証の組合せが複数存在する場合であっても適切な認証の組合せを絞り込むことができる。

【００６４】

具体的には、この認証の選択システムは、制約条件として、図１６に示すように、認証の組合せ方法の優先順位を設定している。この制約条件は、制約条件設定部２２で設定される。目標性能を満たす認証の組合せの候補が複数存在する場合に、認証手段選択部２６で、図１６に示す認証の組合せ方法の優先順位に基づいて配列する。この図１６の例では重み付き線形和の優先順位が最も高いので、まず認証の組合せ方に重み付き線形和を含む組合せを選び、次に優先順位が２番目のＡＮＤ演算を含む組合せを選ぶ。以上のようにして、認証の組合せ方法の優先順位を与えることによって最終候補を絞りこむことができる。なお、制約条件として、組み合わせる認証の数を設定してもよい。

【００６５】

実施の形態６．

本発明の実施の形態６に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態１から５に係る認証の選択システムと比較すると、制約条件として、最終的に選択される認証の組合せの候補数を限定している点で相違する。これによって、設定した候補数以内で認証の組合せを選択するので、迅速に認証の組合せを選択できる。

【００６６】

実施の形態７．

本発明の実施の形態７に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態１に係る認証の選択システムと比較すると、制約条件として認証手段の種類の選択条件を設定する代わりに、あらかじめ使用でき

る認証手段の種類をシステムに接続されている認証手段を識別することによって自動的に行うことができる点で相違する。これによって、選択する認証手段の種類を制約条件として入力しておく必要がなくなり、認証手段の変更を行った場合にも自動的に識別して選択の対象とすることができる。なお、認証手段の識別にあたっては、認証手段である指紋認証装置等を操作することによってセンサの有無を判定し、自動的に識別させてもよい。

【００６７】

実施の形態８.

本発明の実施の形態８に係る認証の選択システムについて説明する。この認証の選択システムは、上記実施の形態１から７に係る認証の選択システムと比較すると、認証手段選択部で認証手段を用いた認証の組み合わせを選択する場合に、制約条件の適用を段階的に行う点で相違する。これによって、認証の組合せの選択を１回で行うのではなく、それぞれ異なる制約条件を別々に適用して総合的に適切な認証の組合せを選択することができる。また、多段階に制約条件を適用することによって認証の組合せを絞り込んで選択してもよい。

【００６８】

【発明の効果】

本発明に係る認証の選択システムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択する認証手段選択部を備えている。これによって、高い認証性能を持つ一の認証又は認証の組合せを適切に選択し、高い精度で認証を行うことができる。

【００６９】

また、本発明に係る認証の選択システムによれば、一の認証又は認証の組合せを生成する組合せ生成部と、生成した一の認証又は認証の組合せの認証性能を演算する複合認証性能演算部とを備えている。これによって各々の認証手段の認証性能から複数の認証手段を用いた認証の組合せ等の認証性能を求めることができる。そこで、一の認証や認証の組合せにおける精度向上の程度を推定することができ、必要な認証性能を備えた一の認証又は認証の組合せを選択できる。

【００７０】

さらに、本発明に係る認証の選択システムによれば、選択する認証に関する制約条件を設定している。これによって、目標性能を満たす認証の組合せが複数存在する場合にも、制約条件に基づいて一の認証又は認証の組合せを選択することができる。

【００７１】

またさらに、本発明に係る認証の選択システムによれば、制約条件として認証手段の種類、認証手段の種類の優先順位等を設定している。これによって、適切な一の認証又は認証の組合せを選択できる。

【００７２】

また、本発明に係る認証の選択システムは、実際の認証のログデータを解析して、各認証手段の認証性能に反映させている。これによって実際の認証実績に応じて適切な一の認証又は認証の組合せを選択することができる。

【００７３】

またさらに、本発明に係る認証の選択システムは、性能記憶部で登録者ごとの認証性能を記憶させている。これによって、各登録者ごとにより適切な認証の組合せを選択することができる。

【００７４】

さらに、本発明に係る認証の選択システムは、認証性能として、被認証者が登録者本人である場合の本人照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうちから選択できる。

【００７５】

本発明に係る認証システムは、上記認証の選択システムと、被認証者を認証する少なくとも一つの認証手段とを備えている。これによって、認証の選択システムで選択した最適な認証の組合せにより、各認証手段を用いた精度の高い認証を行うことができる。

【００７６】

本発明に係る認証の選択方法によれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択している。これによって、選択した一の認証又は認証の組合せによって、高い精度で被認証者を認証することができる。

【００７７】

本発明に係る認証方法によれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択し、選択した一の認証又は認証の組合せによって被認証者を認証している。これによって、高い精度で認証することができる。

【００７８】

本発明に係る認証の選択プログラムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択している。これによって、選択された一の認証又は認証の組合せによって、高い精度で被認証者を認証することができる。

【００７９】

本発明に係る認証の選択プログラムを格納したコンピュータ読取可能な記録媒体によれば、可搬性に優れるので、上記認証の選択システムを容易にコンピュータ上で稼動することができる。

【００８０】

本発明に係る認証プログラムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択し、選択した一の認証又は認証の組合せによって被認証者を認証している。これによって、高い精度で認証することができる。

【００８１】

本発明に係る認証プログラムを格納したコンピュータ読取可能な記録媒体によれば、可搬性に優れるので、上記認証システムを容易にコンピュータ上で稼動することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１に係る認証の選択システム及び認証システムのブロック図である。

【図２】　本発明の実施の形態１に係る認証の選択のフローチャートである。

【図３】　各認証手段の認証性能を演算するフローチャートである。

【図４】　（ａ）は認証手段の認証性能であるＦＲＲ、ＦＡＲと閾値との関係を示すグラフであり、（ｂ）は（ａ）のＦＲＲとＦＡＲをそれぞれ微分して得られる本人照合度分布と他人照合度分布を示すグラフである。

【図５】　（ａ）は本人照合度分布について、設定した閾値による認証の誤り（ＦＲ）との関係を示すグラフであり、（ｂ）は他人照合度分布について、設定した閾値による認証の誤り（ＦＡ）との関係を示すグラフである。

【図６】　図２の各組み合わせの複合認証性能を演算し、記憶する手順１０２の詳細を示すフローチャートである。

【図７】　図６の手順１２７の詳細を示すフローチャートである。

【図８】　図２の手順１０４の詳細を示すフローチャートである。

【図９】　（ａ）は認証の組合せと目標性能を満たす各認証手段の閾値との関係を示す表であり、（ｂ）は（ａ）を制約条件に基づいて並べ替えた表である。

【図１０】　本発明の実施の形態１に係る認証システムによる認証方法のフローチャートである。

【図１１】　本発明の実施の形態２に係る認証の選択システム及び認証システムのブロック図である。

【図１２】　本発明の実施の形態２に係る認証の選択システムにおいて、ログデータのうち、登録者本人と認証されたログデータを本人照合度分布へ反映させる手順のフローチャートである。

【図１３】　本発明の実施の形態２に係る認証の選択システムにおいて、ログデータのうち、登録者本人と認証されたログデータを他人照合度分布へ反映させる手順のフローチャートである。

【図１４】　本発明の実施の形態４に係る認証の選択システムにおいて、認証手段の種類に優先順位を設けた制約条件の表である。

【図１５】　図１４の制約条件に基づいて並べ替えた認証の組合せを示す表である。

【図１６】　本発明の実施の形態５に係る認証の選択システムにおいて、認証の組合せ方法に優先順位を設けた制約条件の表である。

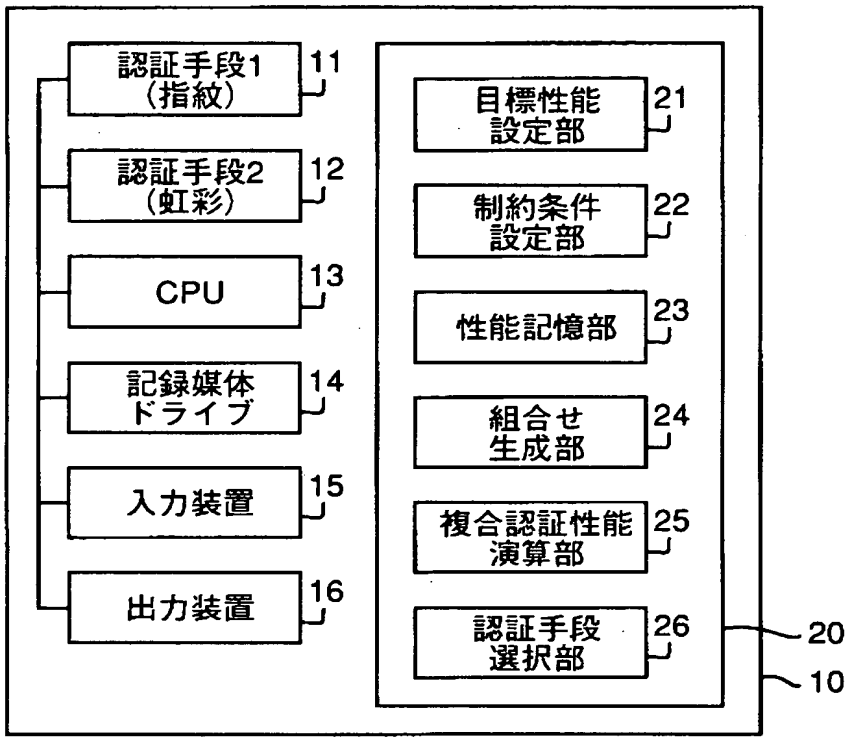
【符号の説明】

１０　認証システム、１１　認証手段１（指紋）、１２　認証手段２（虹彩）、１３　ＣＰＵ、１４　記録媒体ドライブ、１５　入力装置、１６　出力装置、２

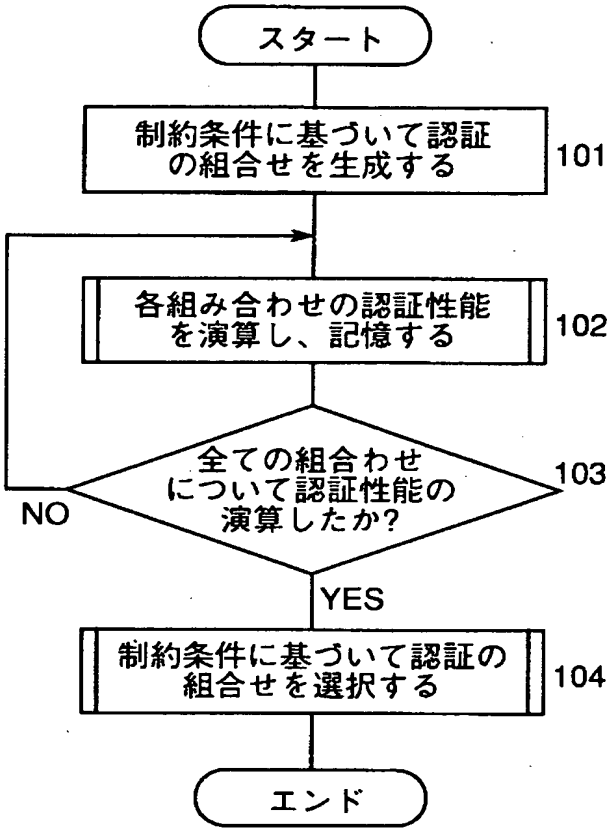
０　メモリ、２１　目標性能設定部、２２　制約条件設定部、２３　性能記憶部、２４　組合せ生成部、２５　複合認証性能演算部、２６　認証手段選択部、２７　ログ解析部

【書類名】　図面

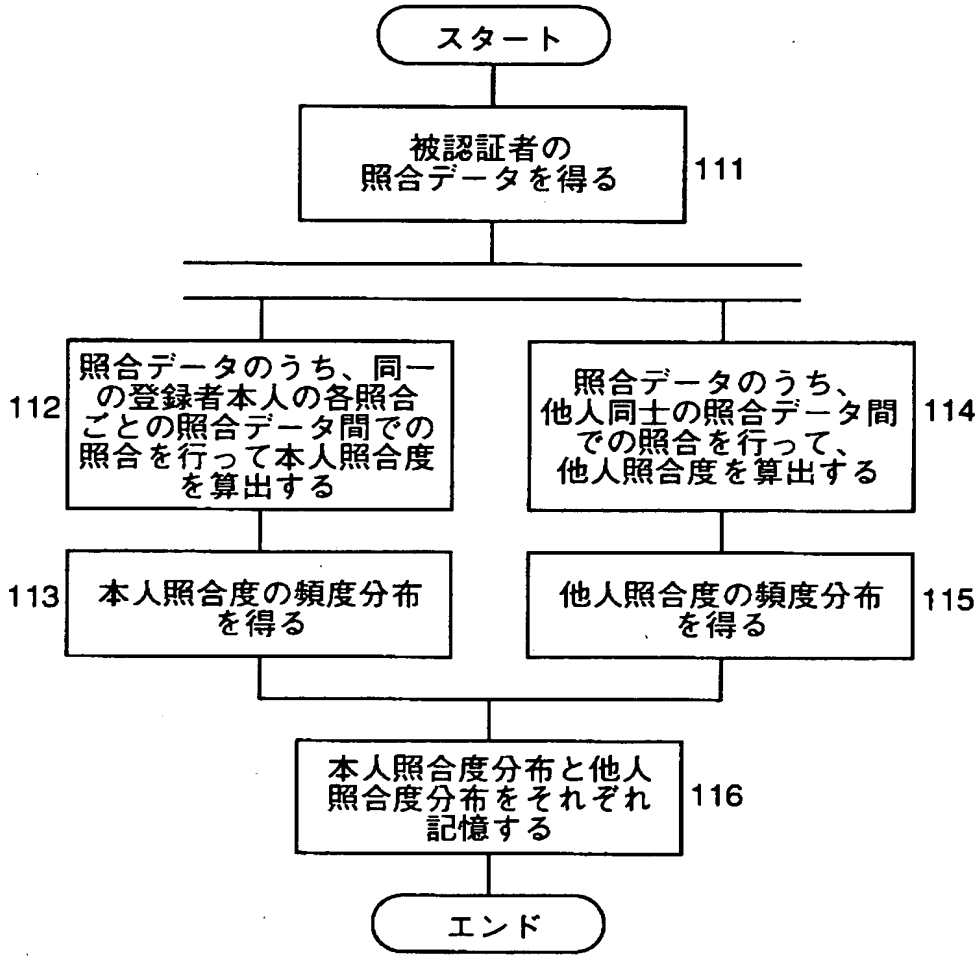
【図１】


認証手段1
(指紋)
11
認証手段2
(虹彩)
12
CPU
13
記録媒体
ドライブ
14
入力装置
15
出力装置
16
目標性能
設定部
21
制約条件
設定部
22
性能記憶部
23
組合せ
生成部
24
複合認証性能
演算部
25
認証手段
選択部
26
20
10

【図２】

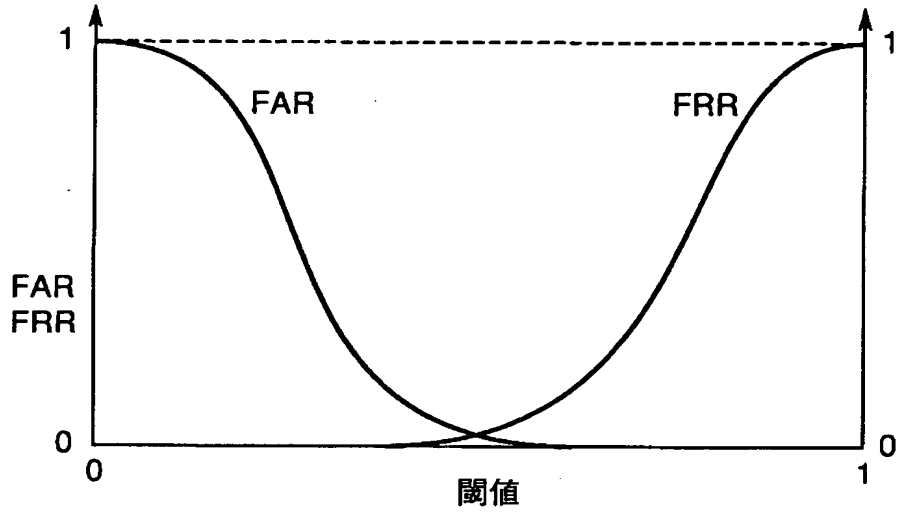

スタート
制約条件に基づいて認証の組合せを生成する
101
各組み合わせの認証性能を演算し、記憶する
102
全ての組合わせについて認証性能の演算したか?
103
NO
YES
制約条件に基づいて認証の組合せを選択する
104
エンド

【図３】

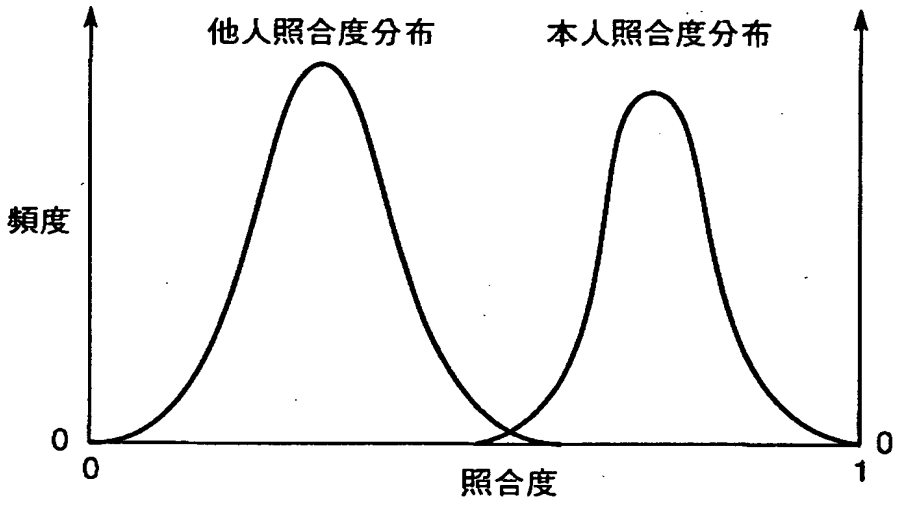

スタート
被認証者の照合データを得る
111
照合データのうち、同一の登録者本人の各照合ごとの照合データ間での照合を行って本人照合度を算出する
112
照合データのうち、他人同士の照合データ間での照合を行って、他人照合度を算出する
114
本人照合度の頻度分布を得る
113
他人照合度の頻度分布を得る
115
本人照合度分布と他人照合度分布をそれぞれ記憶する
116
エンド

【図４】

(a)

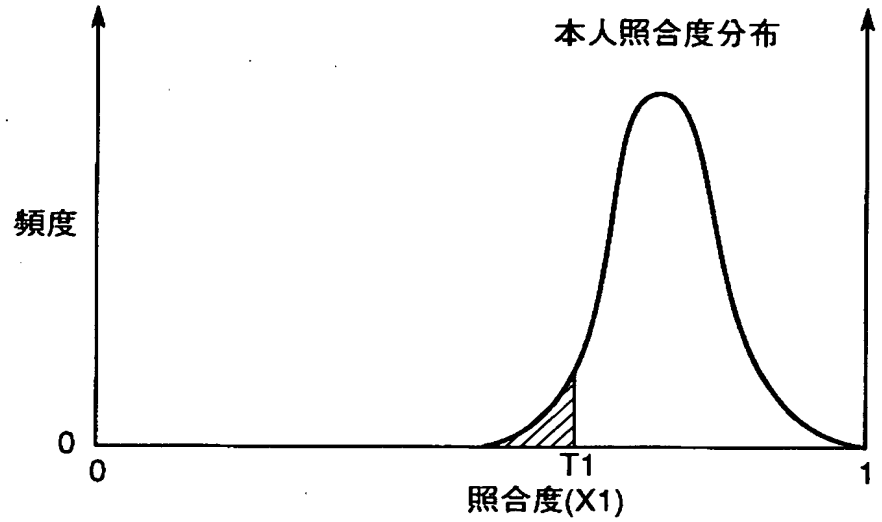


(b)

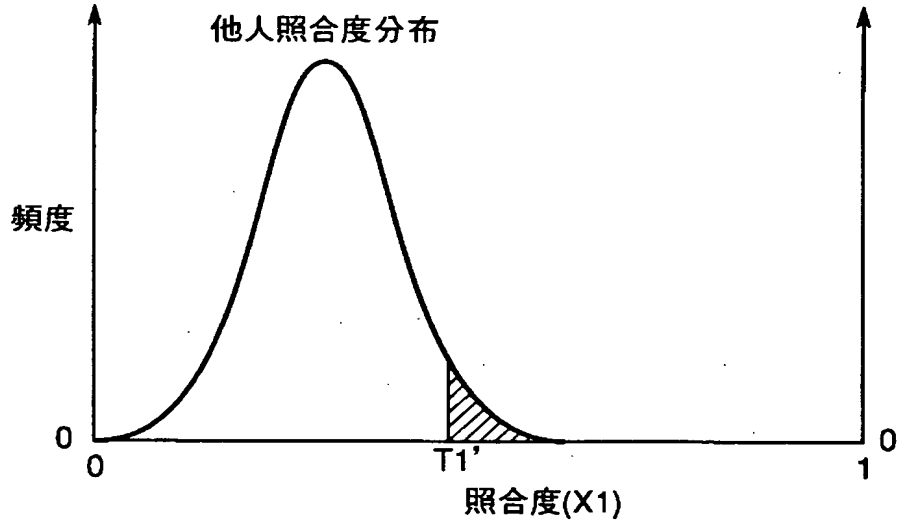


【図５】

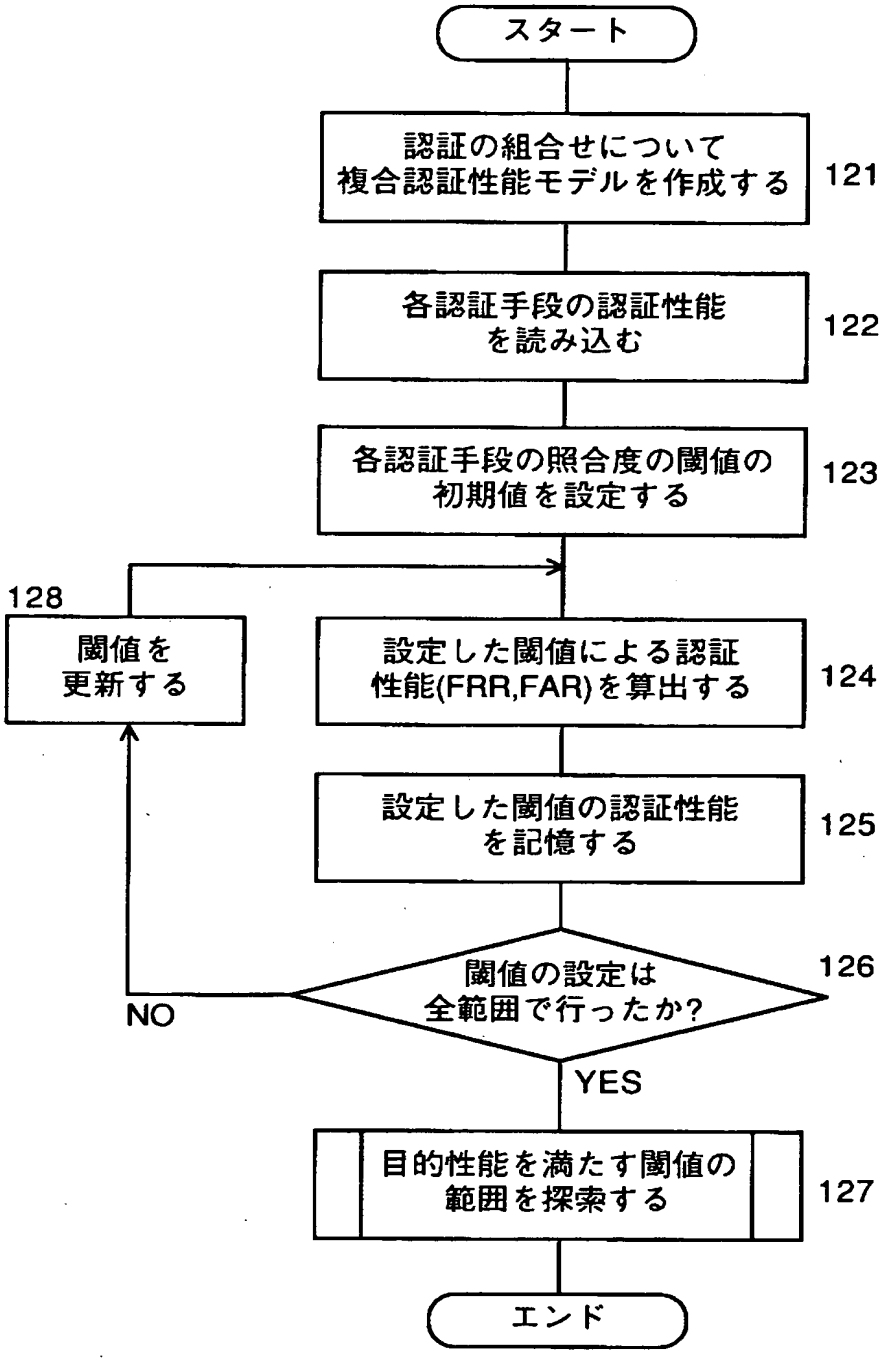
(a)



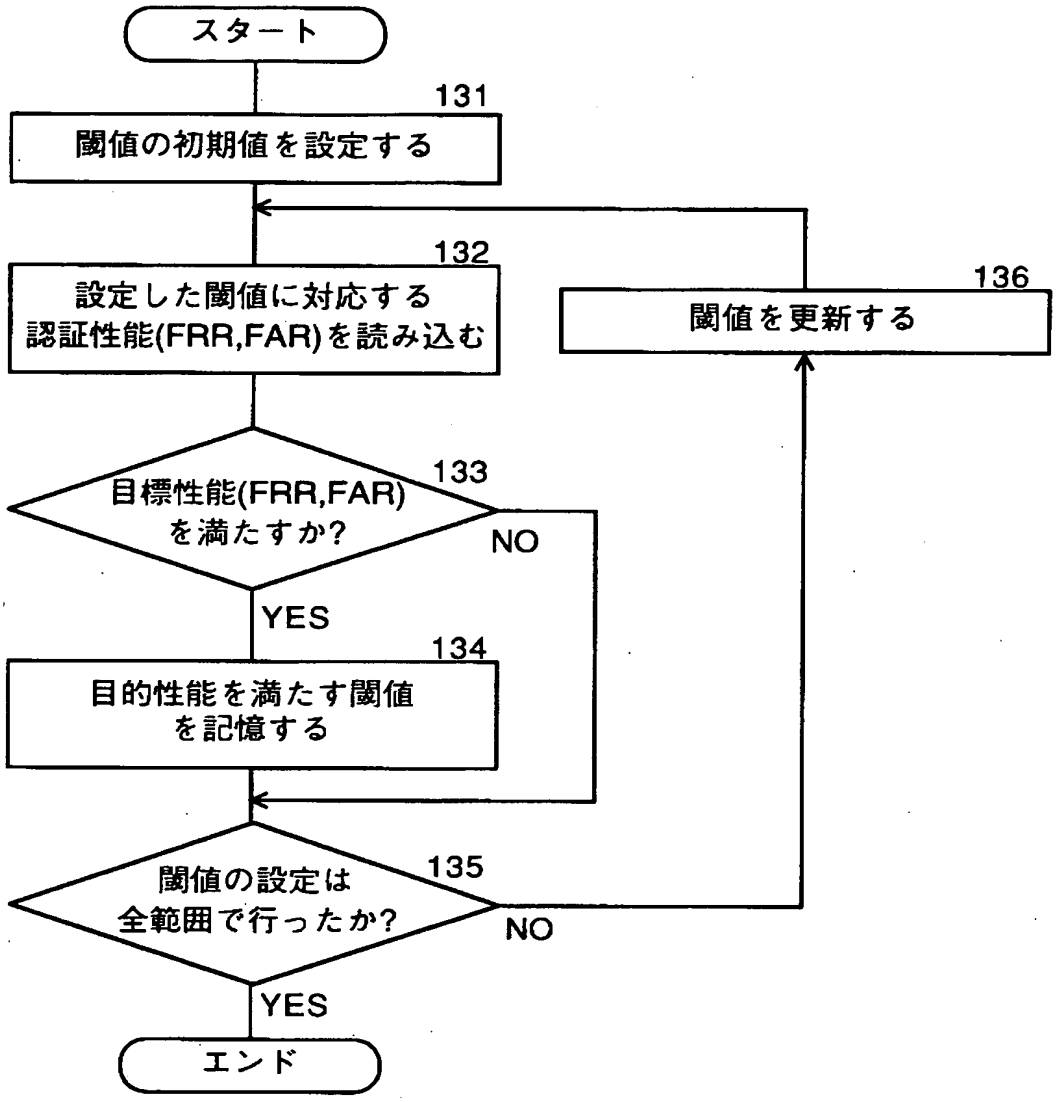
(b)



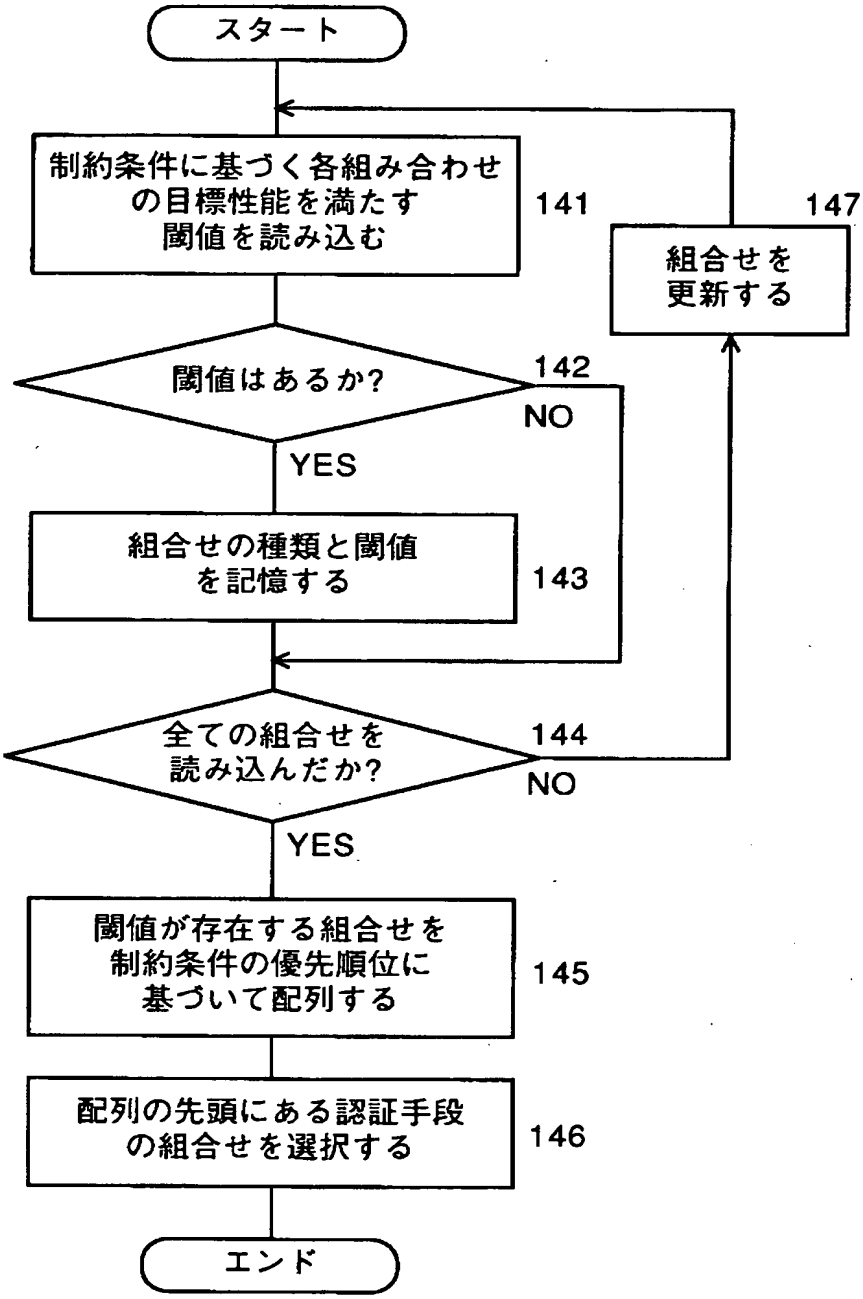
【図６】


スタート
認証の組合せについて
複合認証性能モデルを作成する
121
各認証手段の認証性能
を読み込む
122
各認証手段の照合度の閾値の
初期値を設定する
123
128
閾値を
更新する
設定した閾値による認証
性能(FRR,FAR)を算出する
124
設定した閾値の認証性能
を記憶する
125
閾値の設定は
全範囲で行ったか?
126
NO
YES
目的性能を満たす閾値の
範囲を探索する
127
エンド

【図７】


スタート
131
閾値の初期値を設定する
132
設定した閾値に対応する
認証性能(FRR,FAR)を読み込む
136
閾値を更新する
133
目標性能(FRR,FAR)
を満たすか?
NO
YES
134
目的性能を満たす閾値
を記憶する
135
閾値の設定は
全範囲で行ったか?
NO
YES
エンド

【図８】


スタート
制約条件に基づく各組み合わせの目標性能を満たす閾値を読み込む
141
147
組合せを更新する
閾値はあるか?
142
NO
YES
組合せの種類と閾値を記憶する
143
全ての組合せを読み込んだか?
144
NO
YES
閾値が存在する組合せを制約条件の優先順位に基づいて配列する
145
配列の先頭にある認証手段の組合せを選択する
146
エンド

【図９】

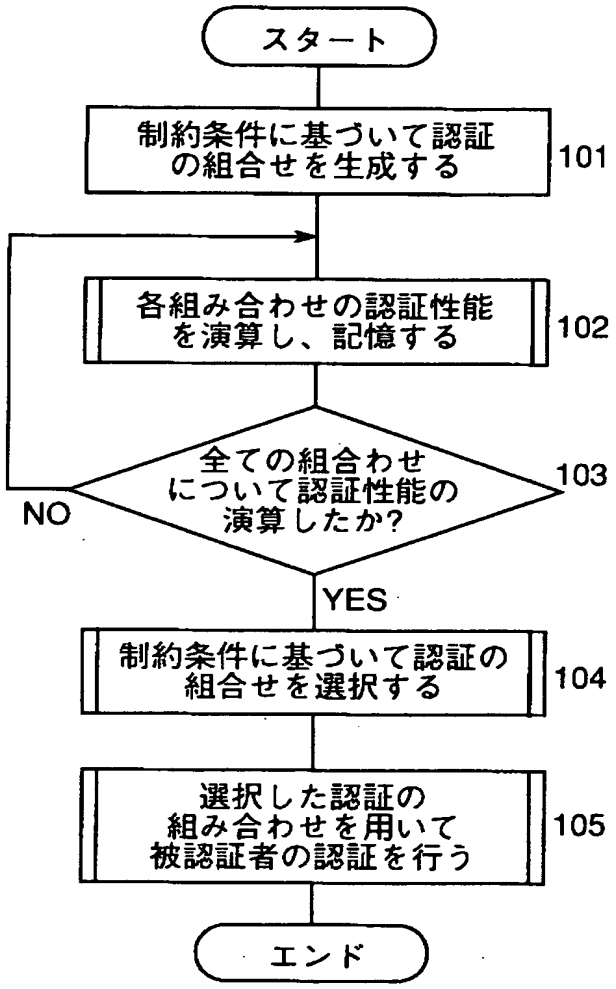
(a)

認証の組合せ	指紋の照合度の閾値（T1）	虹彩の照合度の閾値（T2）
指紋AND指紋AND虹彩AND虹彩	35	40
指紋AND虹彩AND虹彩	40	40
指紋AND指紋AND虹彩	35	45
虹彩AND虹彩	—	50
指紋AND虹彩	55	50
指紋AND指紋	60	—
虹彩	—	55
指紋	なし	—
指紋OR虹彩	なし	なし

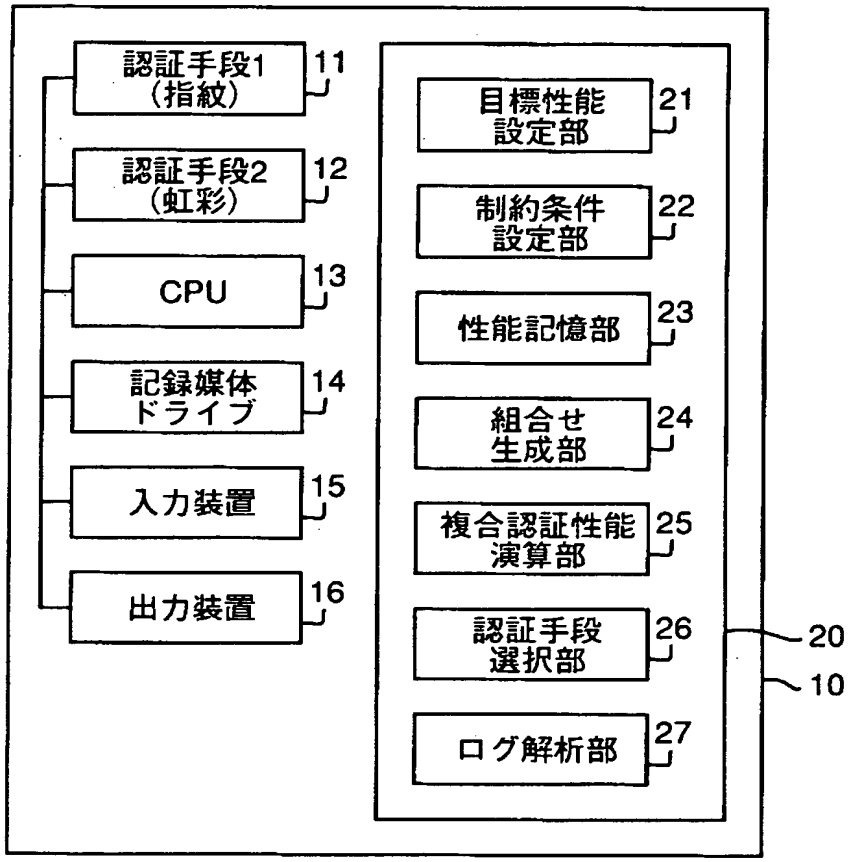
(b)

認証の組合せ	指紋の照合度の閾値（T1）	虹彩の照合度の閾値（T2）
指紋AND指紋	60	—
指紋AND虹彩	55	50
指紋AND指紋AND虹彩	35	45
指紋AND虹彩AND虹彩	40	40
指紋AND指紋AND虹彩AND虹彩	35	40
虹彩	—	55
虹彩AND虹彩	—	50

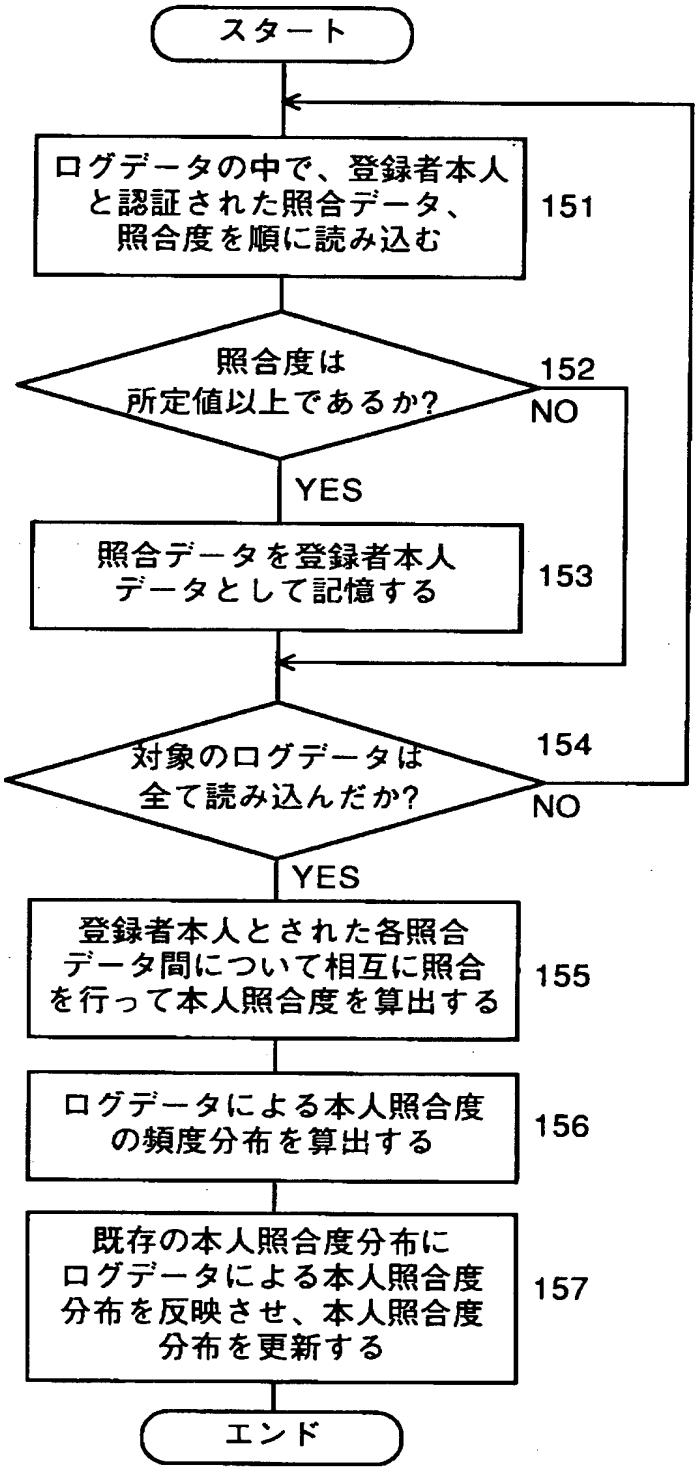
【図１０】


スタート
制約条件に基づいて認証の組合せを生成する
101
各組み合わせの認証性能を演算し、記憶する
102
全ての組合わせについて認証性能の演算したか?
103
NO
YES
制約条件に基づいて認証の組合せを選択する
104
選択した認証の組み合わせを用いて被認証者の認証を行う
105
エンド

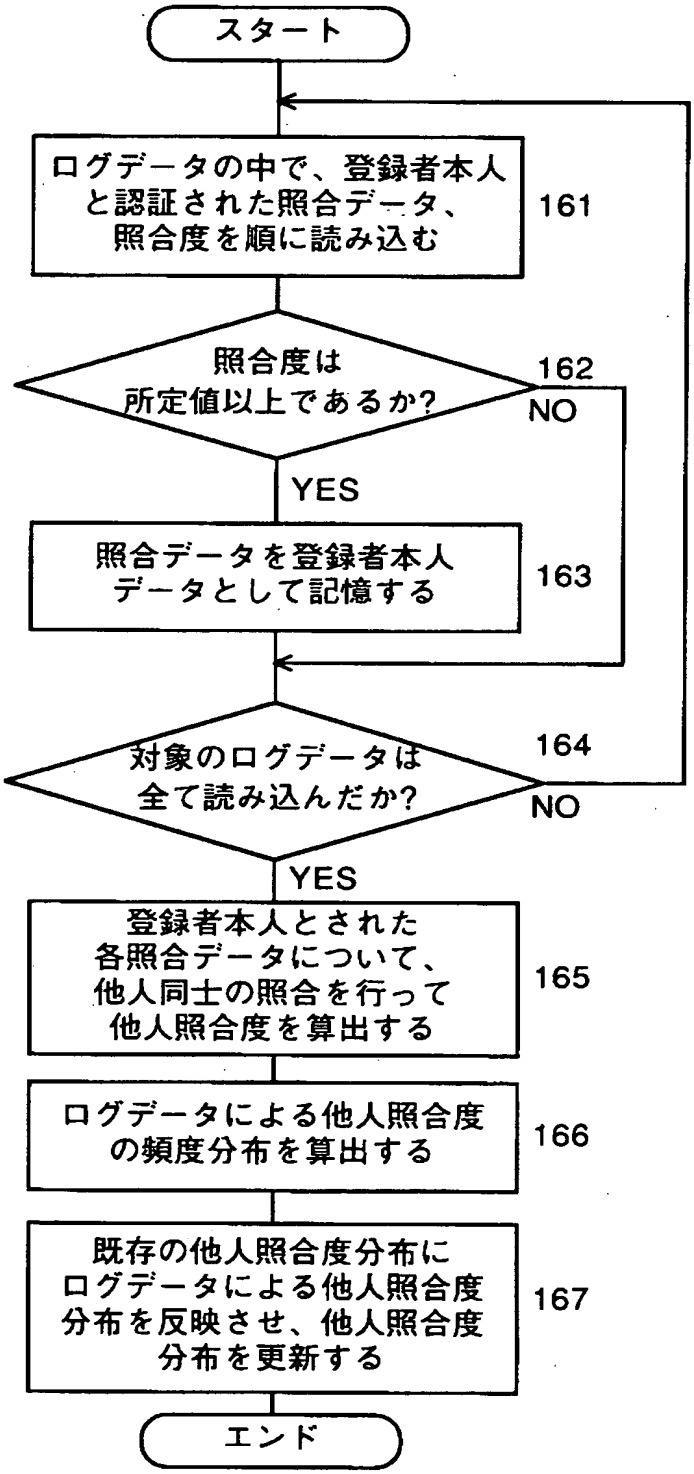
【図１１】


認証手段1
(指紋)
11
認証手段2
(虹彩)
12
CPU
13
記録媒体
ドライブ
14
入力装置
15
出力装置
16
目標性能
設定部
21
制約条件
設定部
22
性能記憶部
23
組合せ
生成部
24
複合認証性能
演算部
25
認証手段
選択部
26
ログ解析部
27
20
10

【図１２】


スタート
ログデータの中で、登録者本人と認証された照合データ、照合度を順に読み込む
151
照合度は所定値以上であるか?
152
NO
YES
照合データを登録者本人データとして記憶する
153
対象のログデータは全て読み込んだか?
154
NO
YES
登録者本人とされた各照合データ間について相互に照合を行って本人照合度を算出する
155
ログデータによる本人照合度の頻度分布を算出する
156
既存の本人照合度分布にログデータによる本人照合度分布を反映させ、本人照合度分布を更新する
157
エンド

【図１３】


スタート
ログデータの中で、登録者本人と認証された照合データ、照合度を順に読み込む
161
照合度は所定値以上であるか?
162
NO
YES
照合データを登録者本人データとして記憶する
163
対象のログデータは全て読み込んだか?
164
NO
YES
登録者本人とされた各照合データについて、他人同士の照合を行って他人照合度を算出する
165
ログデータによる他人照合度の頻度分布を算出する
166
既存の他人照合度分布にログデータによる他人照合度分布を反映させ、他人照合度分布を更新する
167
エンド

【図１４】

優先順位	認証手段の種類
1	指紋
2	虹彩
3	顔

【図１５】

認証の組合せ	指紋の照合度の閾値（T1）	虹彩の照合度の閾値（T2）
指紋AND指紋	60	―
指紋AND指紋AND虹彩	35	45
指紋AND指紋AND虹彩AND虹彩	35	40
指紋AND虹彩	55	50
指紋AND虹彩AND虹彩	40	40
虹彩AND虹彩	―	55
虹彩	―	50

【図１６】

優先順位	認証の組合せ方法
1	重み付き線形和
2	AND
3	OR

【書類名】　　要約書

【要約】

【課題】　認証に要求される目標性能を満たす一の認証又は認証の組み合わせを選択する認証の選択システムを提供する。

【解決手段】　認証の選択システムは、被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部２６を備える。好ましくは、被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組合せを生成する組合せ生成部２４と、前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部２５とをさらに備える。認証システムは、上記認証の選択システムと、被認証者を認証する少なくとも一つの認証手段１１、１２とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　　東京都千代田区丸の内２丁目２番３号
氏　名　　三菱電機株式会社